


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
[Search: The ACM Digital Library The Guide](#)


THE ACM DIGITAL LIBRARY
[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Published before August 2003

Found 1,831 of 145,336

Terms used **command disable signed signature hash**

Sort results by

 Save results to a Binder

[Try an Advanced Search](#)

Display results

 Search Tips

[Try this search in The ACM Guide](#)
 Open results in a new window

Results 1 - 20 of 200

Result page: **1** [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale
1 SMC: a symmetry-based model checker for verification of safety and liveness

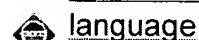

A. Prasad Sistla, Viktor Gyuris, E. Allen Emerson

April 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**,

Volume 9 Issue 2

Publisher: ACM PressFull text available: [pdf\(217.86 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

The article presents the SMC system. SMC can be used for checking safety and liveness properties of concurrent programs under different fairness assumptions. It is based on explicit state enumeration. It combats the state explosion by exploiting symmetries of the input concurrent program, usually present in the form of identical processes, in two different ways. Firstly, it reduces the number of explored states by identifying those states that are equivalent under the symmetries of the syst ...

Keywords: automata, model checking
2 Heraclitus: elevating deltas to be first-class citizens in a database programming


Shahram Ghandeharizadeh, Richard Hull, Dean Jacobs

September 1996 **ACM Transactions on Database Systems (TODS)**, Volume 21 Issue 3**Publisher:** ACM PressFull text available: [pdf\(3.76 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Traditional database systems provide a user with the ability to query and manipulate one database state, namely the current database state. However, in several emerging applications, the ability to analyze "what-if" scenarios in order to reason about the impact of an update (before committing that update) is of paramount importance. Example applications include hypothetical database access, active database management systems, and version management, to name a few. The central th ...

Keywords: active databases, deltas, execution model for rule application, hypothetical access, hypothetical database state

3 COCA: A secure distributed online certification authority

 Lidong Zhou, Fred B. Schneider, Robbert Van Renesse
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4

Publisher: ACM Press

Full text available:  [pdf\(448.28 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no assumption is made about execution speed and message delivery delays; channels are expected to exhibit only intermittent reliability; and with $3t + 1$ COCA servers up to t may be faulty or compromised. COCA is the first system to integr ...

Keywords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

4 Take control of TCPA

David Safford, Jeff Kravitz, Leendert van Doorn
August 2003 **Linux Journal**, Volume 2003 Issue 112

Publisher: Specialized Systems Consultants, Inc.

Full text available:  [html\(21.73 KB\)](#) Additional Information: [full citation](#), [abstract](#)

The free code behind IBM's new security chip. Menace or protector?

5 Separating key management from file system security

 David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review, Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5

Publisher: ACM Press

Full text available:  [pdf\(1.77 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use. We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

6 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5

Publisher: Kluwer Academic Publishers

Full text available:  [pdf\(255.65 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

7 The Satchel system architecture: mobile access to documents and services

Mike Flynn, David Pendlebury, Chris Jones, Marge Eldridge, Mik Lamming
December 2000 **Mobile Networks and Applications**, Volume 5 Issue 4

Publisher: Kluwer Academic Publishers

Full text available: Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index](#)

[pdf\(207.51 KB\)](#)[terms](#)

Mobile professionals require access to documents and document-related services, such as printing, wherever they may be. They may also wish to give documents to colleagues electronically, as easily as with paper, face-to-face, and with similar security characteristics. The Satchel system provides such capabilities in the form of a mobile browser, implemented on a device that professional people would be likely to carry anyway, such as a pager or mobile phone. Printing may be per ...

8 The internet worm program: an analysis



Eugene H. Spafford

January 1989 **ACM SIGCOMM Computer Communication Review**, Volume 19 Issue 1

Publisher: ACM Press

Full text available: [pdf\(2.45 MB\)](#) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

On the evening of 2 November 1988, someone infected the Internet with a *worm* program. That program exploited flaws in utility programs in systems based on BSD-derived versions of UNIX. The flaws allowed the program to break into those machines and copy itself, thus *infecting* those systems. This program eventually spread to thousands of machines, and disrupted normal activities and Internet connectivity for many days. This report gives a detailed description of the components of the ...

9 Termination in language-based systems



Algis Rudys, Dan S. Wallach

May 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 2

Publisher: ACM Press

Full text available: [pdf\(355.43 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Language run-time systems are increasingly being embedded in systems to support run-time extensibility via mobile code. Such systems raise a number of concerns when the code running in such systems is potentially buggy or untrusted. Although sophisticated access controls have been designed for mobile code and are shipping as part of commercial systems such as Java, there is no support for terminating mobile code short of terminating the entire language run-time. This article presents a c ...

Keywords: Applets, Internet, Java, resource control, soft termination, termination

10 Key management and key exchange: A key-management scheme for distributed sensor networks



Laurent Eschenauer, Virgil D. Gligor

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**

Publisher: ACM Press

Full text available: [pdf\(582.21 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Distributed Sensor Networks (DSNs) are ad-hoc mobile networks that include sensor nodes with limited computation and communication capabilities. DSNs are dynamic in the sense that they allow addition and deletion of sensor nodes after deployment to grow the network or replace failing and unreliable nodes. DSNs may be deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitious use by an adversary. Hence DSNs require cryptographic protection of com ...

Keywords: key management, probabilistic key sharing, random graphs, sensor networks

11 A search engine for 3D models

 Thomas Funkhouser, Patrick Min, Michael Kazhdan, Joyce Chen, Alex Halderman, David Dobkin, David Jacobs

January 2003 **ACM Transactions on Graphics (TOG)**, Volume 22 Issue 1

Publisher: ACM Press

Full text available:  pdf(7.91 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

As the number of 3D models available on the Web grows, there is an increasing need for a search engine to help people find them. Unfortunately, traditional text-based search techniques are not always effective for 3D data. In this article, we investigate new shape-based search methods. The key challenges are to develop query methods simple enough for novice users and matching algorithms robust enough to work for arbitrary polygonal models. We present a Web-based search engine system that support ...

Keywords: Search engine, shape matching, shape representation, shape retrieval

12 Design of a high-performance ATM firewall

 Jun Xu, Mukesh Singhal

November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**

Publisher: ACM Press

Full text available:  pdf(1.27 MB)

Additional Information: [full citation](#), [references](#), [index terms](#)

13 Paranoid penguin: detecting suspect traffic

Michael Rash

November 2001 **Linux Journal**, Volume 2001 Issue 91

Publisher: Specialized Systems Consultants, Inc.

Full text available:  html(14.22 KB) Additional Information: [full citation](#), [index terms](#)

14 Invited papers on the frontiers of software practice: Cybersecurity

Richard A. Kemmerer

May 2003 **Proceedings of the 25th International Conference on Software Engineering ICSE '03**

Publisher: IEEE Computer Society

Full text available:   pdf(1.17 MB)  Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)
[Publisher Site](#)

As more business activities are being automated and an increasing number of computers are being used to store sensitive information, the need for secure computer systems becomes more apparent. This need is even more apparent as systems and applications are being distributed and accessed via an insecure network, such as the Internet. The Internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude ...

15 Mobile code: Anomaly intrusion detection in dynamic execution environments

 Hajime Inoue, Stephanie Forrest

September 2002 **Proceedings of the 2002 workshop on New security paradigms NSPW '02**

Publisher: ACM Press

Full text available:  pdf(867.25 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We describe an anomaly intrusion-detection system for platforms that incorporate dynamic compilation and profiling. We call this approach "dynamic sandboxing." By gathering information about applications' behavior usually unavailable to other anomaly intrusion-detection systems, dynamic sandboxing is able to detect anomalies at the application layer. We show our implementation in a Java Virtual Machine is both effective and efficient at stopping a backdoor and a virus, and has a low false positive ...

Keywords: Java, anomaly detection, dynamic sandboxing

16 [Open-Source Intrusion Detection Tools for Linux: Armed with Linux and Open Source tools, you can even keep an ISP secure.](#) 

Bobby S. Wen

October 2000 **Linux Journal**

Publisher: Specialized Systems Consultants, Inc.

Full text available:  html(20.63 KB) Additional Information: [full citation](#), [references](#), [index terms](#)

17 [Risks to the public: Risks to the public in computers and related systems](#) 

 Peter G. Neumann

May 2002 **ACM SIGSOFT Software Engineering Notes**, Volume 27 Issue 3

Publisher: ACM Press

Full text available:  pdf(1.92 MB) Additional Information: [full citation](#)

18 [Risks to the public in computers and related systems](#) 

 Peter G. Neumann

January 1987 **ACM SIGSOFT Software Engineering Notes**, Volume 12 Issue 1

Publisher: ACM Press

Full text available:  pdf(1.91 MB) Additional Information: [full citation](#), [abstract](#)

The RISKS Forum in *Software Engineering Notes* does not limit itself just to software problems (let alone software engineering) because the risks we discuss don't either. Thus the topic demands a broad perspective.

19 [An end-to-end approach to host mobility](#) 

 Alex C. Snoeren, Hari Balakrishnan

August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking MobiCom '00**

Publisher: ACM Press

Full text available:  pdf(1.35 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present the design and implementation of an end-to-end architecture for Internet host mobility using dynamic updates to the Domain Name System (DNS) to track host location. Existing TCP connections are retained using secure and efficient connection migration, enabling established connections to seamlessly negotiate a change in endpoint IP addresses without the need for a third party. Our architecture is secure—name updates are effected via the secure DNS update protocol, while TCP ...

20 [Peer to peer networks: A reputation-based approach for choosing reliable resources in peer-to-peer networks](#) 

 Ernesto Damiani, De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, Fabio Violante

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**

Publisher: ACM Press

Full text available:  [pdf\(650.19 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Peer-to-peer (P2P) applications have seen an enormous success, and recently introduced P2P services have reached tens of millions of users. A feature that significantly contributes to the success of many P2P applications is user anonymity. However, anonymity opens the door to possible misuses and abuses, exploiting the P2P network as a way to spread tampered with resources, including Trojan Horses, viruses, and spam. To address this problem we propose a self-regulating system where the P2P netwo ...

Keywords: peer-to-peer network, polling protocol, reputation-based systems

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)